Purely Cubic Function Fields With Short Periods

R. Scheidler*
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716 USA
scheidle@math.udel.edu

Abstract

A "function field version" of Voronoi's algorithm can be used to compute the fundamental unit of a purely cubic complex congruence function field of characteristic at least 5. This is accomplished by generating a sequence of minima in the maximal order of the field. The number of mimima computed is the period of the field. Generally, the period is very large — it is proportional to the regulator and exponential in the genus of the field — but there are classes of fields with very short periods. For several infinite families of such fields, we explicitly compute the Voronoi continued fraction expansions and the fundamental units. We also investigate the case of period length 1 where the minima in the maximal order are exactly the units of the field. Finally, we explore the connection between regulator and period and other cases of small periods and regulators.

1991 *Mathematics Subject Classification.* Primary 11R16, 11R27. Secondary 11R58, 11Y65.

Key Words and Phrases. Purely cubic function field, Fundamental unit, Regulator, Voronoi's algorithm, Period

*Research supported by NSF grant DMS-9631647

1 Introduction

Voronoi's algorithm [7], [1, pp. 273–304] computes the fundamental unit of a complex cubic number field by generating the "Voronoi continued fraction expansion" of the unit. An explicit implementation in purely cubic fields was given by Williams et al. [9], and Williams' version was adapted to purely cubic congruence function fields of characteristic at least 5 and unit rank 1 in [4, 5]. In short, the method produces a chain $(\theta_n)_{n \in \mathbb{N}}$ of successive minima in the maximal order of the field by starting with $\theta_1 = 1$ and computing adjacent minima θ_n of increasing absolute value such that $\theta_{n+1} = \mu_n \theta_n$ and μ_n is the minimum adjacent to 1 in the reduced fractional principal ideal $\mathfrak{a}_n = (\theta_n^{-1})$ $(n \in \mathbb{N})$. If $l \in \mathbb{N}$ is the first index such that θ_{l+1} has constant norm, then θ_{l+1} is the fundamental unit of positive degree of the field, and l is the period of the fundamental unit (or of the field).

Usually, l is exponentially large in the genus of the field, but in fields with very small fundamental units, the period is as small as linear in the genus of the field. In [3], the fundamental units for a number of infinite classes of such fields were explicitly given. In all these fields, the generating polynomial of the field is of the form $D = (M^3 - F)/E^3$ where E, F, M are polynomials such that E^3 divides $M^3 - F$ and F divides M^2. In this paper, we determine the periods of several infinite subfamilies of these fields. We should point out that similar investigations were previously performed for purely cubic number fields with short periods in [8]. We also analyze the situation of small periods and regulators; in particular, the case where the period is 1. This setting is of particular interest because here, the fundamental unit is the minimum adjacent to 1 in the maximal order of the field, and moreover, the minima θ_n $(n \in \mathbb{N})$ in the Voronoi chain are exactly the units in the field.

A general introduction to function fields can be found in [6]; the purely cubic case is discussed in considerable detail in [2] and [4, 5]. Let $k = \mathbb{F}_q$ be a finite field of order q whose characteristic is not 3. If t is a transcendental element over k, denote by $k[t]$ and $k(t)$ the ring of polynomials and the field of rational functions, respectively, over k in the variable t. Let $D \in k[t]$ be a nonconstant cubefree polynomial and let ρ be a fixed cube root of D in some algebraic closure of $k(t)$. Then the other cube roots of D are $u\rho$ and $u^2\rho$ where u is a primitive cube root of unity which lies in an algebraic extension of k of degree at most 2. The cubic extension $K = k(t, \rho)$ of $k(t)$

is a *purely cubic (congruence) function field* over the *field of constants* k. The *maximal order* of K is the integral closure $\mathcal{O} = \overline{k[t]}$ of $k[t]$ in K. $\mathcal{O}$ is both a ring and a $k[t]$-module of rank 3; a *(t)-integral basis* of K is a $k[t]$-basis of $\mathcal{O}$ (which consequently is also a $k(t)$-basis of K). If $D = GH^2$ where $G, H \in k[t]$ are both squarefree and relatively prime, then an integral basis of K is is given by $\{1, \rho, \omega\}$ where ρ is as before and $\omega = \rho^2/H$. We have $\rho^3 = D$ and $\omega^3 = \overline{D}$ where $\overline{D} = G^2H$. ω is also a generator of K over $k(t)$, and in the corresponding integral basis, one simply has to reverse the roles of ρ and ω. We point out that in contrast to the number field case, it is a simple matter to determine H from D; namely $H = \gcd(D, D')$ where D' is the formal derivative of D with respect to t. The bases $\{1, \rho, \rho^2\}$ and $\{1, \omega, \omega^2\}$ generate submodules $\mathcal{O}_\rho$ and $\mathcal{O}_\omega$ of $\mathcal{O}$, respectively. $\mathcal{O}_\rho = \mathcal{O}$ if and only if $D = G$ is squarefree and $\mathcal{O}_\omega = \mathcal{O}$ if and only if $D = H^2$ is a square.

The *conjugates* of an element $\alpha = A + B\rho + C\omega \in K$ $(A, B, C \in k(t))$ are $\alpha' = A + Bu\rho + Cu^2\omega$ and $\alpha'' = A + Bu^2\rho + Cu\omega$. The *norm* and *trace* of α *(over* $k(t)$*)* are the respective quantities

$$\begin{array}{rclcl} N(\alpha) & = & \alpha\alpha'\alpha'' & = & A^3 + B^3GH^2 + C^3G^2H - 3ABCGH, \\ Tr(\alpha) & = & \alpha + \alpha' + \alpha'' & = & 3A. \end{array}$$

We have $N(\alpha), Tr(\alpha) \in k(t)$, and if $\alpha \in \mathcal{O}$, then $N(\alpha), Tr(\alpha) \in k[t]$.

The group $\mathcal{O}^*$ of (t-)units of $\mathcal{O}$ is an Abelian group whose torsion part is the group of nozero constants k^*. Its rank is the *(t-)unit rank* of K and a set of generators of the torsion-free part is a system of *fundamental (t-)units* of K. If $\alpha \in \mathcal{O}$, then $N(\alpha) \in k^*$ if and only if α is a unit in $\mathcal{O}$. Depending on the form of q and D, the unit rank can be 0, 1, or 2 (see [4] for details); this is in contrast to purely cubic number fields, which are complex cubic fields and thus always have unit rank 1. In [4], it was shown that a purely cubic function field is *complex*, i.e. has unit rank 1, if and only if $q \equiv 2 \pmod 3$, the degree $\deg(D)$ of D is a multiple of 3, and the leading coefficient $\operatorname{sgn}(D)$ of D is a cube in k^*. Then k does not contain any primitive cube roots of unity, so if $\alpha \in K$, then $\alpha', \alpha'' \notin K$, but $\alpha'\alpha'' = N(\alpha)\alpha^{-1} \in K$. Under these conditions, K can embedded in the field $k((1/t))$ of *Puiseux series* over k. Nonzero elements in $k((1/t))$ are of the form $\alpha = \sum_{i=m}^{\infty} a_i/t^i \in k((1/t))$ $(m \in \mathbb{Z}$, $a_i \in k$ for $i \geq m$, $a_m \neq 0)$. Denote by

$$\deg(\alpha) \quad = \quad -m \text{ the } \textit{degree} \text{ of } \alpha,$$

$$\begin{aligned} |\alpha| &= q^{\deg(\alpha)} = q^{-m} \text{ the } \textit{(absolute) value} \text{ of } \alpha, \\ \operatorname{sgn}(\alpha) &= a_m \text{ the } \textit{sign} \text{ of } \alpha, \\ \lfloor \alpha \rfloor &= \sum_{i=m}^{0} \frac{a_i}{t^i} \text{ the } \textit{principal part} \text{ of } \alpha. \end{aligned}$$

We also set $\deg(0) = -\infty$, $|0| = 0$, and $\lfloor 0 \rfloor = 0$. Note that $\lfloor \alpha \rfloor \in k[t]$ and $|\alpha - \lfloor \alpha \rfloor| < 1$ for any $\alpha \in k((1/t))$. If $\alpha \in K$, then we let $\deg(\alpha') = \deg(\alpha'') = \deg(\alpha'\alpha'')/2$ and $|\alpha'| = |\alpha''| = \sqrt{|\alpha'\alpha''|} = q^{\deg(\alpha')}$.

Henceforth, we assume K to be a purely cubic complex function field. Then we have one fundamental unit ϵ of positive degree that is unique up to factors in k^*. The *(t-)regulator* of K is the positive integer $R = \deg(\epsilon)/2 = -\deg(\epsilon')$. The *genus* of K is $g = \deg(GH) - 2$.

To make this paper somewhat self-contained, we briefly review Voronoi's algorithm as described in [4] in the next section. The case of period length 1 is analyzed in section 3 and connections between the regulator and the period as well as instances of small periods are explored in section 4.

2 Voronoi's Algorithm

Recall that a subset $\mathfrak{a}$ of $\mathcal{O}$ is an *integral ($\mathcal{O}$-)ideal* if for any $\alpha, \beta \in \mathfrak{a}$ and $\theta \in \mathcal{O}$, $\alpha + \beta \in \mathfrak{a}$ and $\theta\alpha \in \mathfrak{a}$. A subset $\mathfrak{a}$ of K is a *fractional ($\mathcal{O}$-)ideal* if there exists a nonzero polynomial $d \in k[t]$ such that $d\mathfrak{a}$ is an integral ideal of $\mathcal{O}$. Henceforth, we assume all ideals to be nonzero, so the term "ideal" will be synonymous with "nonzero ideal". Every fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is a $k[t]$-module of rank 3; if $\{\lambda, \mu, \nu\}$ is a $k[t]$-basis of $\mathfrak{a}$ ($\lambda, \mu, \nu \in K$), write $\mathfrak{a} = [\lambda, \mu, \nu]$. A fractional ideal $\mathfrak{a}$ is *principal* if $\mathfrak{a}$ is of the form $\mathfrak{a} = \{\theta\alpha \mid \theta \in \mathcal{O}\}$ for some $\alpha \in K$; write $\mathfrak{a} = (\alpha)$.

If $\mathfrak{a}$ is a fractional ideal and $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, then α is a *minimum* in $\mathfrak{a}$ if for nonzero $\beta \in \mathfrak{a}$, $|\beta| \leq |\alpha|$ and $|\beta'| \leq |\alpha'|$ imply $\beta \in k^*\alpha$, i.e. β and α differ only by a nonzero constant factor. $\mathfrak{a}$ is *reduced* if $1 \in \mathfrak{a}$ and 1 is a minimum in $\mathfrak{a}$. $\mathcal{O}$ is reduced, and in fact every unit in $\mathcal{O}$ is a minimum in $\mathcal{O}$. Let $\mathfrak{a}$ be a fractional ideal and let $\theta \in \mathfrak{a}$ be a minimum in $\mathfrak{a}$. An element $\phi \in \mathfrak{a}$ is a *minimum adjacent to θ in* $\mathfrak{a}$ if ϕ is a minimum in $\mathfrak{a}$, $|\theta| < |\phi|$, and for no $\alpha \in \mathfrak{a}$, $|\theta| < |\alpha| < |\phi|$ and $|\alpha'| < |\theta'|$. ϕ always exists and is unique up to a trivial unit factor, so we will henceforth speak of *the* minimum adjacent to an element in a fractional ideal, keeping in mind that it is only unique up to a trivial unit factor. If $\mathfrak{a}$ is a fractional ideal and $\theta = \theta_1$ is a minimum in $\mathfrak{a}$, then a sequence $(\theta_n)_{n \in \mathbb{N}}$ of elements in $\mathfrak{a}$ where θ_{n+1} is the minimum adjacent to θ_n in $\mathfrak{a}$ $(n \in \mathbb{N})$ is a *chain of successive minima in* $\mathfrak{a}$.

The basic idea for Voronoi's algorithm is as follows. Start with the reduced ideal $\mathfrak{a}_1 = \mathcal{O}$ and the minimum $\theta_1 = 1$ in $\mathfrak{a}_1$. Define a sequence of reduced fractional ideals $\mathfrak{a}_n$ and minima $\theta_n \in \mathcal{O}$ $(n \in \mathbb{N})$ as follows. Let μ_n be the minimum adjacent to 1 in $\mathfrak{a}_n$ and set $\theta_{n+1} = \mu_n \theta_n$, $\mathfrak{a}_{n+1} = \mu_n^{-1}\mathfrak{a}_n = (\theta_{n+1}^{-1})$. Then it can be shown that θ_{n+1} is the minimum adjacent to θ_n in $\mathcal{O}$ and $\mathfrak{a}_{n+1}$ is a reduced fractional ideal. Thus, we have a chain of successive minima in $\mathcal{O}$ given by

$$(\theta_n)_{n \in \mathbb{N}} \quad \text{where} \quad \theta_1 = 1, \quad \theta_n = \prod_{i=1}^{n-1} \mu_i \text{ for } n \geq 2. \tag{2.1}$$

This chain can be shown to contain in fact all the minima in $\mathcal{O}$ of nonnegative degree, so in particular, the fundamental unit ϵ of K must appear in the chain. Specifically, if $l \in \mathbb{N}$ is the first index such that $N(\theta_{l+1})$ is constant, then θ_{l+1} is equal to ϵ up to a constant factor. l is the *period* of ϵ (or of K). Since $\mathfrak{a}_{ml+i} = \mathfrak{a}_i$ and $\mu_{ml+i} = \mu_i$ for all $m, i \in \mathbb{N}$, the sequence (2.1) is equal to

$$1, \theta_2, \ldots, \theta_l, \epsilon, \epsilon\theta_2, \ldots, \epsilon\theta_l, \epsilon^2, \epsilon^2\theta_2, \ldots, \epsilon^3, \ldots$$

and contains all nonpositive powers of ϵ. We note that $l = 1$ if and only if (2.1) consists exactly of all the nonpositive powers of ϵ; that is, every minimum in $\mathcal{O}$ is a unit in $\mathcal{O}$ and vice versa.

The chain (2.1) is computed as follows. Each ideal $\mathfrak{a}_n = (\theta_n^{-1})$ will be given in terms of a *reduced* $k[t]$-basis $\{1, \mu_n, \nu_n\}$ that satisfies certain bounds and includes the minimum μ_n adjacent to 1 in $\mathfrak{a}_n$. The basis elements μ_n and ν_n are of the form $\mu_n = (M_{0n} + M_{1n}\rho + M_{2n}\omega)/U_n$, $\nu_n = (N_{0n} + N_{1n}\rho + N_{2n}\omega)/U_n$ where $M_{0i}, N_{0i}, U_n \in k[t]$ for $i = 0, 1, 2$. Then $\theta_{n+1} = \mu_n \theta_n$ and $\mathfrak{a}_{n+1} = \mu_n^{-1}\mathfrak{a}_n = [1, 1/\mu_n, \nu_n/\mu_n]$. We now replace this basis of $\mathfrak{a}_{n+1}$ by a new reduced $k[t]$-basis $\{1, \mu_{n+1}, \nu_{n+1}\}$ where μ_{n+1} is the minimum adjacent to 1 in $\mathfrak{a}_{n+1}$. This is accomplished by applying a sequence of suitable unimodular transformations to the pair $(1/\mu_n, \nu_n/\mu_n)$ of basis elements of $\mathfrak{a}_{n+1}$, until we obtain the reduced basis. Details on how to compute such a basis will be given below. We then go on to compute θ_{n+2}. The process terminates once a basis denominator U_{n+1} that is constant is encountered, in which case

$\mathfrak{a}_{n+1} = \mathcal{O}$ and $\theta_{n+1} = \epsilon$ (up to a constant factor), i.e. $n = l$. The following algorithm computes the fundamental unit ϵ of K. In each iteration, the current value of θ_n is $(E_0 + E_1\rho + E_2\omega)/V$.

Algorithm 2.1 (Fundamental Unit Algorithm) *Input: The polynomials G, H where $D = GH^2$.*

Output: $E_0, E_1, E_2 \in k[t]$ where $\epsilon = E_0 + E_1\rho + E_2\omega$ is the fundamental unit of K.

Algorithm:

1. *Set $E_0 = V = M_1 = N_2 = U = 1$, $E_1 = E_2 = M_0 = M_2 = N_0 = N_1 = 0$. (So $\theta_1 = 1$, $\mu = \rho$, $\nu = \omega$.)*
2. *Repeat*
   - *(a)* { Reduce the basis }
     Use Algorithm 2.2 below to replace $M_0, M_1, M_2, N_0, N_1, N_2, U$ by the coefficients of a reduced basis;
   - *(b)* { Update θ_n }
     - *i. Replace*

       $$\begin{pmatrix} E_0 \\ E_1 \\ E_2 \\ V \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} E_0M_0 + (E_1M_2 + E_2M_1)GH \\ E_0M_1 + E_1M_0 + E_2M_2G \\ E_0M_2 + E_1M_1H + E_2M_0 \\ UV \end{pmatrix};$$

     - *ii. Compute $S = \gcd(E_0, E_1, E_2, V)$. For $i = 0, 1, 2$, replace E_i by E_i/S and V by V/S;*
   - *(c)* { Update μ and ν }
     - *i. Set*

       $$\begin{aligned} A_0 &= M_0^2 - M_1M_2GH, \\ A_1 &= M_2^2G - M_0M_1, \\ A_2 &= M_1^2H - M_0M_2, \\ B &= M_0^3 + M_1^3GH^2 + M_2^3G^2H - 3M_0M_1M_2GH \ = \ N(\mu); \end{aligned}$$

```
    ii. Replace
            $\begin{pmatrix} M_0 \\ M_1 \\ M_2 \end{pmatrix}$ by $\begin{pmatrix} A_0U \\ A_1U \\ A_2U \end{pmatrix}$;
    iii. Replace
            $\begin{pmatrix} N_0 \\ N_1 \\ N_2 \end{pmatrix}$ by $\begin{pmatrix} A_0N_0 + (A_1N_2 + A_2N_1)GH \\ A_0N_1 + A_1N_0 + A_2N_2G \\ A_0N_2 + A_1N_1H + A_2N_0 \end{pmatrix}$;
    iv. Replace $U$ by $B$;
    v. Compute $S = \gcd(M_0, M_1, M_2, N_0, N_1, N_2, U)$. For $i = 0, 1, 2$,
       replace $M_i$ by $M_i/S$, $N_i$ by $N_i/S$ and $U$ by $U/S$;
until $U \in k^*$.
```

We now tackle the problem of computing a reduced basis and, in particular, the minimum μ_{n+1} adjacent to 1 in the reduced fractional ideal $\mathfrak{a}_{n+1}$ ($n \in \mathbb{N}_0$). Henceforth, we need to exclude the characteristic 2 case, that is, we require k to be a finite field of characteristic at least 5. Let $\alpha = A + B\rho + C\omega \in K$ with $A, B, C \in k(t)$. We define the quantities

$$\begin{array}{rcl} \xi_\alpha & = & B\rho + C\omega, \\ \eta_\alpha & = & B\rho - C\omega, \\ \zeta_\alpha & = & 2A - B\rho - C\omega. \end{array} \tag{2.2}$$

We call a basis $\{1, \mu, \nu\}$ of a reduced fractional ideal *reduced* if

$$|\zeta_\mu| < 1, \ |\zeta_\nu| < 1, \ |\xi_\mu| > |\xi_\nu|, \ |\eta_\mu| < 1 \leq |\eta_\nu|. \tag{2.3}$$

If $\{1, \mu, \nu\}$ is a reduced basis of $\mathfrak{a}$, then it can be shown that μ is the minimum adjacent to 1 in $\mathfrak{a}$. The following algorithm produces on input of any basis of a reduced fractional ideal a reduced basis of that same ideal.

Algorithm 2.2 (Reduction Algorithm)

Input: A basis $\{1, \tilde{\mu}, \tilde{\nu}\}$ *of a reduced fractional ideal* $\mathfrak{a}$.

Output: A reduced basis $\{1, \mu, \nu\}$ of $\mathfrak{a}$.

Algorithm:

1. *Set $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.*

2. *If $|\xi_\mu| < |\xi_\nu|$ or if $|\xi_\mu| = |\xi_\nu|$ and $|\eta_\mu| < |\eta_\nu|$, replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix};$$

3. *If $|\eta_\mu| \geq |\eta_\nu|$*

   (a) *while $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor \eta_\mu/\eta_\nu \rfloor$, replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix};$$

   (b) *Replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix};$$

   (c) *If $|\eta_\mu| = |\eta_\nu|$, replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$$

   where $a = sgn(\eta_\mu) sgn(\eta_\nu)^{-1} \in k^*$;

4. (a) *While $|\eta_\nu| < 1$, replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix};$$

   (b) *While $|\eta_\mu| \geq 1$, replace*

   $$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} \lfloor \eta_\nu/\eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix};$$

5. *If $|\zeta_\mu| \geq 1$, replace μ by $\mu - (1/2)\lfloor \zeta_\mu \rfloor$;*
   If $|\zeta_\nu| \geq 1$, replace ν by $\nu - (1/2)\lfloor \zeta_\nu \rfloor$.

3 The Case of Minimal Period

Of particular interest is the situation where the period $l = 1$, in which case ϵ is the minimum adjacent to 1 in $\mathcal{O}$ and can be computed using one iteration of Algorithm 2.2.

Lemma 3.1 *If α is an element in some reduced fractional ideal, then $|N(\alpha)| > |GH|^{-2}$.*

Proof: See Corollary 4.7 of [4]. □

Lemma 3.2 *Let $\mathfrak{a}$ be a reduced fractional ideal of $\mathcal{O}$ and let $\alpha \in \mathfrak{a}$. Then there exists a minimum $\theta \in \mathfrak{a}$ such that $|\theta| \leq |\alpha|$ and $|\theta'| \leq |\alpha'|$.*

Proof: The claim is clear if α is itself a minimum, so suppose α is not a minimum in $\mathfrak{a}$. Then the set $H(\alpha) = \{\beta \in \mathfrak{a} \mid |\beta| \leq |\alpha|,\ |\beta'| \leq |\alpha'|,\ \beta \notin k^*\alpha\}$ is not empty. Let $\beta \in H(\alpha)$, then by Lemma 3.1 $\deg(\beta) = \deg(N(\beta)) - 2\deg(\beta') > -2(\deg(GH) + \deg(\alpha'))$. Thus, the set $\{\deg(\beta) \mid \beta \in H(\alpha)\}$ is a nonempty subset of the integers that is bounded below. By the Well-Ordering Principle, this set has a smallest element. Let $\theta \in H(\alpha)$ be of minimal degree, that is, $|\theta| \leq |\alpha|$, $|\theta'| \leq |\alpha'|$, $\theta \notin k^*\alpha$, and for any $\beta \in H(\alpha)$, $|\beta| \geq |\theta|$.

We claim that θ is a minimum in $\mathfrak{a}$. To see this, let $\beta \in \mathfrak{a}$, $\beta \neq 0$, with $|\beta| \leq |\theta|$ and $|\beta'| \leq |\theta'|$. Then $|\beta| \leq |\alpha|$ and $|\beta'| \leq |\alpha'|$. If $\beta \in k^*\alpha$, then $|\beta| = |\alpha| \geq |\theta|$. If $\beta \notin k^*\alpha$, then $\beta \in H(\alpha)$, so $|\beta| \geq |\theta|$. Either way, $|\beta| = |\theta|$.

Let $\gamma = \beta - \mathrm{sgn}(\beta)\mathrm{sgn}(\theta)^{-1}\theta$, then $|\gamma| < |\theta| \leq |\alpha|$, so $\gamma \notin k^*\alpha$. Also $|\gamma'| \leq \max\{|\beta'|, |\theta'|\} \leq |\alpha'|$. Since $|\gamma| < |\theta|$, γ cannot lie in $H(\alpha)$. The only way this is possible is if $\gamma = 0$, so $\beta \in k^*\theta$. □

For the remainder of this section, we again assume that $\mathrm{char}(k) \geq 5$.

Theorem 3.3 *If $l = 1$ and $|G| > |H|$, then $D = M^3 - a$ for some $M \in k[t]$ and $a \in k^*$.*

Proof: Suppose $|G| > |H|$. Then $|\rho^3| = |GH^2| < |G^2H| = |\omega|^3$, so $|\rho| < |\omega|$. Let $\alpha = \lfloor \rho \rfloor - \rho \in \mathcal{O}$, then $|\alpha| < 1$ and since $\alpha'\alpha'' = \lfloor \rho \rfloor^2 + \lfloor \rho \rfloor \rho + \rho^2$,

$|\alpha'| = |\rho|$. Also $N(\alpha) = \lfloor\rho\rfloor^3 - D$. If α is a minimum in $\mathcal{O}$, then α is a unit in $\mathcal{O}$ since $l = 1$. In this case, $D = M^3 - a$ with $M = \lfloor\rho\rfloor \in k[t]$ and $a = N(\alpha) \in k^*$. Suppose now that α is not a minimum in $\mathcal{O}$. By Lemma 3.2, there exists a minimum $\theta \in \mathcal{O}$ with $|\theta| \leq |\alpha|$ and $|\theta'| \leq |\alpha'|$. Then θ is also a unit in $\mathcal{O}$.

Let $\theta = A + B\rho + C\omega$ with $A, B, C \in k[t]$. Then $A \neq 0$, as otherwise GH would divide the constant $N(\theta)$. Since $|\theta| \leq |\alpha| < 1$, we must have $|\theta'| > 1$ because 1 is a minimum in $\mathcal{O}$. Hence

$$\begin{array}{rclcccccc} |A| & = & |\theta + \theta' + \theta''| & \leq & |\theta'| & \leq & |\alpha'| & = & |\rho|, \\ |B\rho + C\omega| & = & |\alpha - A| & = & |A| & \leq & |\rho|, & & \\ |B\rho - C\omega| & = & |\theta' - \theta''| & \leq & |\theta'| & \leq & |\rho|. & & \end{array}$$

Thus $|B\rho|, |C\omega| \leq |\rho|$. This implies $|B| \leq 1$, so $B \in k$. Also $|C\rho| < |C\omega| \leq |\rho|$ implies $|C| < 1$, so $C = 0$, and since $|\theta| < 1$, $B \neq 0$, so $B \in k^*$. Since $N(\theta) = A^3 + B^3 D$, we have $D = M^3 - a$ with $M = -B^{-1}A \in k[t]$ and $a = -B^{-3}N(\theta) \in k^*$. □

Lemma 3.4 *If $D = M^3 - a$ with $M \in k[t]$ and $a \in k^*$, then $|G| > |M| > |H|$.*

Proof: Suppose $|G| \leq |H|$, then $|M|^3 = |GH^2| \leq |H|^3$, so $|M| \leq |H|$. Taking the derivative of the equality $GH^2 = M^3 - a$ shows that H divides $M^2 M'$. Since $\gcd(H, M) = 1$, this implies that H divides M', so $|M| \leq |H| \leq |M'| < |M|$, a contradiction. Hence $|G| > |H|$ and $|M|^3 = |GH^2| > |H|^3$, implying $|M| > |H|$ and $|G| = |M|^3/|H|^2 > |M|$. □

Lemma 3.5 *If $D = M^3 - a$ with $M \in k[t]$ and $a \in k^*$, then the fundamental unit of K is $\epsilon = M^2 + M\rho + \rho^2$.*

Proof: It is easier to prove that $\delta = M - \rho = (a(M^2 + M\rho + \rho^2))^{-1}$ is the fundamental unit of negative degree of K. To that extent, let $\delta = \eta^s$ where $\eta = A + B\rho + C\omega \in \mathcal{O}$ is the fundamental unit of K of negative degree and $s \in \mathbb{N}$. Then

$$|\eta'| = |\delta'|^{1/s} = |\delta'\delta''|^{1/2s} = |\delta|^{-1/2s} = |M^2 + M\rho + \rho^2|^{1/2s} = |M|^{1/s}.$$

Now a simple calculation shows

$$\begin{aligned} B &= \frac{1}{3\rho}(\eta + u^2\eta' + u\eta''), \\ C &= \frac{1}{3\omega}(\eta + u\eta' + u^2\eta''), \end{aligned}$$

where we recall that u is a primitive cube root of unity in some algbraic closure of k. Since $|\rho| = |M|$ and $|\rho^2| = |H\omega| \geq |\omega|$, we have

$$\begin{aligned} |B| &\leq \frac{|\eta'|}{|\rho|} \leq \frac{|M|^{\frac{1}{s}}}{|\rho|} = |M|^{\frac{1}{s}-1}, \\ |C| &\leq \frac{|\eta'|}{|\omega|} \leq \frac{|M|^{\frac{1}{s}}}{|\rho|^2} = |M|^{\frac{1}{s}-\frac{1}{2}}. \end{aligned}$$

If $B \neq 0$, then $1/s - 1 \geq 0$, implying $s = 1$ and $\eta = \delta = M - \rho$. Suppose $B = 0$, then $C \neq 0$ as otherwise $\eta = A$ and $|\eta| < 1$ together imply a contradiction. In this case, $1/s - 1/2 \geq 0$, so $s \leq 2$. Suppose $s = 2$, then comparing coefficents of ω in $(A + C\omega)^2 = M - \rho$ yields $2AC = 0$. Since $\text{char}(k) \neq 2$, we must have $A = 0$, implying the contradiction $1 > |\eta| = |C\omega|$. □

Theorem 3.6 *If $D = M^3 - a$ with $M \in k[t]$ and $a \in k^*$, then $l = 1$.*

Proof: If $D = M^3 - a$, then $\gcd(M, H) = 1$, so there exist polynomials $X, Y \in k[t]$ with $|Y| < |H|$ and $HX - MY = 1$. Set $\mu = M^2 + M\rho + H\omega = M^2 + M\rho + \rho^2$, $\nu = \lfloor X\rho + Y\omega \rfloor/2 + X\rho + Y\omega$. Then μ, $\nu \in \mathcal{O}$ and $\{1, \mu, \nu\}$ is a basis of $\mathcal{O}$. Since μ is the fundamental unit of K by Lemma 3.5, we see that $l = 1$ if μ is the minimum adjacent to 1 in $\mathcal{O}$, so it suffices to show that μ and ν satisfy conditions (2.3). Using Lemma 3.4, we obtain

$$\begin{aligned} |\zeta_\mu| &= |2M - M\rho - \rho^2| = |(2M + \rho)(M - \rho)| \\ &= \frac{|2M + \rho|}{|M^2 + M\rho + \rho^2|} = \frac{1}{|M|} < 1, \\ |\zeta_\nu| &= |\lfloor X\rho + Y\omega \rfloor - (X\rho + Y\omega)| < 1, \\ |\xi_\mu| &= |M\rho + \rho^2| = |M|^2, \\ |\xi_\nu| &= |X\rho + Y\omega| = \frac{|\rho|}{|H|}|HX + Y\rho| = \frac{|M|}{|H|}|MY + 1 + Y\rho| \end{aligned}$$

$$
\begin{aligned}
&= \frac{|M|}{|H|}|MY| \ < \ |M|^2 \ = \ |\xi_\mu|, \\
|\eta_\mu| \ &= \ |M\rho - \rho^2| \ = \ |\rho||M-\rho| \ = \ \frac{1}{|M|} \ < \ 1, \\
|\eta_\nu| \ &= \ |X\rho - Y\omega| \ = \ \frac{|\rho|}{|H|}|HX - Y\rho| \\
&= \ \frac{|M|}{|H|}|Y(M-\rho)+1| \ > \ |Y(M-\rho)+1| = 1,
\end{aligned}
$$

where the last equality follows from $|Y(M-\rho)| = |Y|/|M^2 + M\rho + \rho^2| < |H|/|\rho|^2 = |\omega|^{-1} < 1$. So μ and ν satisfy (2.3) and hence $l = 1$. □

Lemma 3.4 and the previous two theorems establish the following:

Corollary 3.7
$l = 1$ and $|G| > |H|$ if and only if $D = M^3 - a$ for some $M \in k[t]$ and $a \in k^*$.
$l = 1$ and $|G| < |H|$ if and only if $\overline{D} = M^3 - a$ for some $M \in k[t]$ and $a \in k^*$.

In the case where $l = 1$ and $|G| = |H|$, there is no simple description of D analogous to that given in the above corollary. We will see below that if both G and H are linear, then $l = 1$ always. On the other hand, there are instances where G and H are of the same degree and not linear, and $l = 1$ for any field of constants k. $G = t^2 + 1$ and $H = t^2$ yields one such example. We also point out that the possibility $|G| = |H|$ can never occur in a purely cubic number field $K = \mathbb{Q}(\sqrt[3]{D})$ as in this case $D = \pm G^3$ would be a cube in $\mathbb{Z}$.

4 Small Periods And Regulators

In general, the regulator R of a purely cubic complex function field of characteristic $\neq 3$ can be very large; up to exponentially large in the genus $g = \deg(GH) - 2$ of K.

Proposition 4.1 *$R \leq (\sqrt{q}+1)^{2g}$, so $R \leq q^g + O(q^{g-1/2}) = \dfrac{|GH|}{q^2} + O\left(\dfrac{|GH|}{q^{5/2}}\right)$.*

Proof: We have $R \leq L(1)$ where $L(u) = \prod_{i=1}^{2g}(1 - \lambda_i u)$ is the L-polynomial of K. Here, the λ_i are algebraic numbers such that $|\lambda_i| = \sqrt{q}$ for $1 \leq i \leq 2g$ by the Hasse-Weil Theorem (see [6, Theorem V.1.15, p. 166, and Theorem V.2.1, p. 169]). □

Henceforth, we assume once again that $\mathrm{char}(k) \geq 5$. Then the period l and the regulator R of K are closely related and are in fact proportional, so large regulators will result in large period lengths and vice versa.

Proposition 4.2 $\dfrac{2R}{\deg(GH)} \leq l \leq 2R.$

Proof: We have $2R = \deg(\epsilon) = \deg(\theta_{l+1}) = \sum_{i=1}^{l} \deg(\mu_i)$. Since each μ_i is the minimum adjacent to 1 in some reduced fractional ideal, we have $|\mu_i| > 1$ for all $i \in \mathbb{N}$. On the other hand $|\mu_i| \leq |GH|$ for all $i \in \mathbb{N}$ by Theorem 7.6 of [4]. It follows that $l \leq \deg(\theta_{l+1}) \leq l \deg(GH)$, so $l \leq 2R$ and $l \geq 2R/\deg(GH)$. □

We should point out that in almost all the computations performed in [4], the values of l and R were very close together and often differed only by 1. We anayze the relationship between regulator and period more closely when these values are very small.

Proposition 4.3 *If $l = 1$, then $R \leq \dfrac{1}{3}\max\{\deg(D), \deg(\overline{D})\}$. If $\deg(D) \neq \deg(\overline{D})$, or equivalently, $|G| \neq |H|$, then equality holds.*

Proof: Suppose $l = 1$. If $|G| > |H|$, then by Corollary 3.7 $D = M^3 - a$ with $a \in k^*$ and $M \in k[t]$. By Lemma 3.5, $\epsilon = M^2 + M\rho + \rho^2$ and $R = \deg(M) = \deg(D)/3 > \deg(\overline{D})/3$. If $|G| < |H|$, then by Corollary 3.7 $\overline{D} = M^3 - a$ with $a \in k^*$ and $M \in k[t]$. Here, we can apply Lemma 3.5 with the roles of ρ and ω exchanged, so we obtain $\epsilon = M^2 + M\omega + \omega^2$ and $R = \deg(M) = \deg(\overline{D})/3 > \deg(D)/3$. Finally, if $|G| = |H|$, then by Proposition 4.2 $R \leq \deg(GH)/2 = \deg(G) = \deg(D)/3 = \deg(\overline{D})/3$. □

Proposition 4.4 $R = 1$ *if and only if* $l = 1$ *and* $\deg(D) = 3$ *or* $\deg(\overline{D}) = 3$.

Proof: By [3], $R = 1$ if and only if $D = M^3 - a$ or $D = (M^3 - a)^2$ or $D = GH^2$ with $a \in k^*$, $M \in k[t]$, and $\deg(M) = \deg(G) = \deg(H) = 1$.

If $D = M^3 - a$ with $\deg(M) = 1$, then $\deg(D) = 3$, and D is squarefree as any square polynomial divisor of D would have to divide both $M^3 - a$ and M^2. Hence by Corollary 3.7 $l = 1$. If $D = (M^3 - a)^2$, then D is a square, so $G = 1$, $H = M^3 - a = \overline{D}$, $\deg(\overline{D}) = 3$, and $l = 1$ by Corollary 3.7. If $D = GH^2$ with linear G and H, then $\deg(D) = 3$, and one iteration of Voronoi's Algorithm shows that $l = 1$ and $\epsilon = (b^2 + GH) + (G - b)\rho + (H + b)\omega$ where $b = (G - H)/3 \in k^*$.

Conversely, suppose $l = 1$ and $\deg(D) = 3$ or $\deg(\overline{D}) = 3$. If $\deg(D) = 3$, then either $\deg(G) = \deg(H) = 1$ or $\deg(G) = 3$ and $\deg(H) = 0$. In the former case, $R = 1$ by the remark at the beginning of the proof. In the latter case, $D = M^3 - a$ with $a \in k^*$ and $M \in k[t]$ by Corollary 3.7. Then M must be linear, so $R = 1$, again by the remark at the beginning of the proof. If $\deg(\overline{D}) = 3$, then either $\deg(G) = \deg(H) = 1$ or $\deg(G) = 0$ and $\deg(H) = 3$. In the former case, once again $R = 1$. In the latter case, $\overline{D} = M^3 - a$ with $a \in k^*$ and $M \in k[t]$ by Corollary 3.7. Again, M is linear. Then $D = (M^3 - a)^2$, so by the above remark, $R = 1$. □

We conclude this paper with some more instances of small periods. This investigation was inspired by [8], where several classes of purely cubic number fields with small periods were analyzed; namely fields of the type $K = \mathbb{Q}(\sqrt[3]{D})$ where $D \in \mathbb{Z}$ is squarefree and is of the form $D = m^3 + a$ or $D = m^3 + am$ with $m \in \mathbb{Z}$ and $a = \pm 1$ or ± 3. As in the number field case, the task of finding the period length of a purely cubic complex function field $K = k(t, \sqrt[3]{D})$ where D is not squarefree is much more difficult than the corresponding problem for squarefree radicands. We were able to establish the periods of two infinite families of fields with squarefree D analogous to those analyzed by Williams [8]. Our results were obtained by applying Voronoi's algorithm to these fields.

Proposition 4.5 *Let $D = M^3 - aM$ where $M \in k[t]$, $a \in k^*$, and D is squarefree. Then $l = 2$. The fundamental unit of K is*

$$\epsilon = (9M^4 - 9M^2 + 1) + 3M(3M^2 - 2)\rho + 3(3M^2 - 1)\rho^2$$

and the regulator of K is $R = 2\deg(M)$. The reduced bases computed in *each step of Algorithm 2.1 are given as follows:*

$$\begin{aligned}
\mu_1 &= M(3M^2 - 2a) + (3M^2 - a)\rho + 3M\rho^2, \\
\nu_1 &= \left(M^2 - \frac{a}{2}\right) + M\rho + \rho^2, \\
\mu_2 &= \frac{M^2 + M\rho + \rho^2}{M}, \\
\nu_2 &= \frac{M\rho - \rho^2}{M}.
\end{aligned}$$

Proposition 4.6 *Let $D = M^3 - F$ where $M, F \in k[t]$, $1 < |F| < |M|$, F divides M, and D is squarefree. Then $l = 3$. The fundamental unit of K is*

$$\epsilon = \left(9\left(\frac{M^3}{F}\right)^2 - 9\frac{M^3}{F} + 1\right) + 3\frac{M^2}{F}\left(3\frac{M^3}{F} - 2\right)\rho + 3\frac{M}{F}\left(3\frac{M^3}{F} - 1\right)\rho^2$$

and the regulator of K is $R = \deg(M^3/F) = \deg(D) - \deg(F)$. The reduced bases computed in each step of Algorithm 2.1 are given as follows:

$$\begin{aligned}
\mu_1 &= M^2 + M\rho + \rho^2, & \nu_1 &= M/2 + \rho, \\
\mu_2 &= \frac{M^2 + M\rho + \rho^2}{F}, & \nu_2 &= \frac{M/2 + \rho}{F}, \\
\mu_3 &= \frac{M^2 + M\rho + \rho^2}{F} = \mu_2, & \nu_3 &= M/2 + \rho = \nu_1.
\end{aligned}$$

References

[1] B. N. Delone and D. K. Fadeev, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs **10**, Amer. Math. Soc., Providence, Rhode Island 1964.

[2] M. Mang, *Berechnung von Fundamentaleinheiten in algebraischen, insbesondere rein-kubischen Kongruenzfunktionenkörpern*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, Germany 1987.

[3] R. Scheidler, *Purely Cubic Complex Function Fields With Small Units*, Submitted to *Acta Arithmetica.*

[4] R. Scheidler and A. Stein, *Voronoi's Algorithm in Purely Cubic Congruence Function Fields of Unit Rank 1*, submitted to *Math. Comp.*

[5] R. Scheidler and A. Stein, *Unit Computation in Purely Cubic Function Fields of Unit Rank 1*, to appear in *Proceedings of the Third Algorithmic Number Theory Symposium ANTS-III*, *Lecture Notes in Computer Science* **1423**, Springer-Verlag, Berlin 1998.

[6] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin 1993.

[7] G. F. Voronoi, *On a Generalization of the Algorithm of Continued Fractions* (in Russian), Doctoral Dissertation, Warsaw, Poland 1896.

[8] H. C. Williams, The period length of Voronoi's algorithm for certain cubic orders, *Publicationes Mathematicae Debrecen* **37**, 1990, pp. 245–265.

[9] H. C. Williams, G. Cormack and E. Seah, Calculation of the regulator of a pure cubic field, *Math. Comp.* **34**, 1980, pp. 567–611.